# Security Implications of ICT Adoption in the High Courts of Malaysia

Ani Munirah Mohamad, Zaiton Hamin, and Mohd Bahrin Othman

***Abstract*—Bearing in mind the double-edged nature of information and communication technology (ICT), it is admitted that at one end, ICT introduces great possibilities and benefits, at the other end, it inevitably leads to various uncertainties and insecurities. It is within this context that this paper aims to critically examine the security implications of ICT in the High Courts of Malaysia. In addition, this research aims to propose recommendations for the amendment to the relevant statutes, improvement to the practice directions and to propose best practices and code of conduct in implementing ICT in the courts. Drawn from an ongoing research which attempts to examine the legal implications of the current adoption of ICT on the delivery of the civil justice system of the High Courts in Malaysia, the research adopts a qualitative method, comprising of the collection of primary data (which involves a field work adopting the case study design) and secondary data (which involves a library-based research). The primary data which have been generated is analysed by using the computer-aided qualitative data analysis software ATLAS.ti version 6.2 prior to reporting of the same. The paper concludes that the adoption of ICT in these courts are imbued with numerous security implications, which in many ways would challenge the way the judicial business would be carried out and also the way in which justice would be delivered and served.**

***Index Terms*—Security implications, information and communication technologies, ICT adoption, e-Court, e-Justice**

## I. Introduction

In line with the understanding that the information and communication technology (ICT) is double-edged in nature, many researchers admit that the ICT adoption by the courts come with speed and efficiency, but cautions that there are security issues that are yet to be resolved (West, 2002; Bhatt, 2005). Accordingly, this paper discusses the ongoing research on the security implications raised by ICT in the civil justice system of the High Courts in Malaysia. The first section discusses the research problem of the study, highlighting the research question, the research objectives and the scope of the research. The second section describes the research methodology that is chosen for this study, followed by the third section which reviews the literatures on the concept and applications of ICT in the Malaysian courts and its relative security implications. This paper concludes with the preliminary findings of the study.

Manuscript received April 13, 2012; revised May 23, 2012.

A. M. Mohamad is with College of Law, Government and International Studies, Universiti Utara Malaysia and Faculty of Law, Universiti Teknologi MARA Shah Alam, Malaysia

Z. Hamin is with Accounting Research Institute HiCoE and Faculty of Law, Universiti Teknologi MARA Shah Alam, Malaysia

M. B. Othman is with Students' Development Division and Faculty of Law, Universiti Teknologi MARA Shah Alam, Malaysia

## II. Research Question and Objectives

The research question of the study is: what security implications does the current adoption of ICT have on the delivery of the civil justice system of the High Courts in Malaysia? Consequently, there are two objectives to this research; the first is to critically examine the security implications of ICT in the civil justice system of the High Courts in Malaysia. Second, this research aims to propose recommendations for the amendment to the Rules of High Court 1980 and relevant Statutes, improvement to the practice directions, and to propose best practices and code of conduct in implementing ICT at the courts.

## III. Methodology

This research adopts a qualitative method, which engages in both the primary and the secondary data. The collection of the primary data involves a field work in which the data are generated from two case studies that focuses on two units of analysis representing the High Courts in West Malaysia i.e. High Court in Kuala Lumpur, and another being the High Court in East Malaysia i.e. High Court in Kuching, Sarawak. The units of analysis for the case study are described in Fig 1.


Fig. 1. The units of analysis for the case study.

The instrument used is face-to-face semi-structured interview with respondents who are involved directly with the application of ICT at each of the courts, being the judge, the court officer, the system developer, the legal practitioner, and the client. In total, twelve respondents of the primary data are interviewed. The interviews enquired into the perception of the respondents on relevant issues including their involvement in the technology adoption at the courts, the security risks of the application of ICT at the courts, and

how do they cope with the risks at hand. The interviews are then analysed using ATLAS.ti qualitative data analysis software before the research findings are prepared.

The second part of the research involves the collection of secondary data (including both primary and secondary sources) by way of library based research. Primary sources include the relevant laws affecting civil trials in Malaysia while secondary sources include documents collected from the respondents during the semi-structured interviews, policies of the Federal and State governments and the judiciary, the rulings of the Malaysian Bar Council, the state bars, practice directions and online databases.

## IV. ICT Adoption in the High Courts of Malaysia

There are currently six technology applications which are adopted at the High Courts in Kuala Lumpur and in Kuching Sarawak, namely the e-filing system, case management system, queue management system, court recording and transcription, audio and video conference system and the integrated community and advocates' portal. Each of the systems is briefly discussed below.

First, the e-filing application allows for electronic submission of court documents for the purpose of filing and registration by the litigants and/or their solicitors using the Internet. For this purpose, the users are provided with an online account and security password to be used when dealing with the e-filing process (Hamidah, 2011). Second, case management system (CMS) is a system software that manages all cases managed by the court through the computer system. It allows for the computerization of court processes, retrieval of information online, easy monitoring of performance, and generates statistics automatically, which in turn, would lead to some uniformity in reporting (CMS Briefing, 2010).

Third, the queue management system (QMS) is available for case management area and hearings before the registrars. Under this system, numerous kiosks were placed within the court complex to facilitate the attendance of the lawyers for the particular cases.. Fourth, the court recording and transcription (CRT) system consists of video and audio recording both in open court and chambers hearings. As for the case at the High Court in Kuala Lumpur, the recordings will be kept in the courts database and controlled by the interpreter during the proceedings (Nik Imran, 2011).

Fifth, the audio conference system is used at both the High Courts of Kuala Lumpur and Sarawak for court hearings among judges, lawyers and other persons involved in the session despite being at different locations. Hence, judges and lawyers can save time and money travelling to and fro and out of town (Zaki, 2010). Sixth and final, the community and advocates' portal (CAP) serves as an information technology channel of communication and operations among the public community, including the clients, the advocates who represent them and the judiciary.

## V. The Security Implications

Zaiton (2009) contended that the use of technologies could facilitate many computer crimes or computer-related crimes including hacking, denial of service, phishing, pharming, identity theft, computer fraud and stalking. On this note, Aldridge, White and Forcht (1997), Bhimani (1996), Furnell and Karweni (1999) and Gefen (2000) examined such security risks along the lines of the basic security control requirements of authentication, non-repudiation, privacy protection, confidentiality and data integrity. Each of the risks is discussed below in light of the ICT adoption in the High Courts of Malaysia.

## VI. The Authentication Risks

Authentication is an important requirement for security as it determines that the communicating or transacting parties are who they claim to be. It is undeniable that for the best functioning of technological transactions all parties should be able to feel comfortable that they are communicating with the party whom they think they are doing business with (Bhimani, 1996). The parties engaging in the ICT applications could run the risk that they might be communicating with an unintended counterpart, especially for the case of e-filing, AVC and the ICAP.

### *A. The Non-Repudiation Risks*

The requirement of non-repudiation ensures that neither of the party involved in a transaction should be able to deny having participated in the transaction after the fact. It provides some assurance of the origin or the delivery of the data in order to protect the sender against false denial by the recipient that the data has actually been received, as well as to protect the recipient against false denial by the sender that the data has actually been sent (Chong, 1998). This requirement would well be relevant to each of the ICT applications in the courts.

### *B. The Privacy Protection Risks*

In the context of e-commerce, Suh and Han (2003) contends that privacy protection would be pertinent as it would ensure that personal information about customers collected from their electronic transactions is protected from any disclosure without their permission. Within the context of the courts, although privacy protection is essential, the public's right to access the court records is widely debated as scrutinized by FitzGerald (1989-1990), Blankley (2004) and Salzmann (2000). The conflict between the public's right to access the court records is even more complex with the advent of the ICT into the court system, as these new technologies introduce more complex features and functions of record and information keeping and processing by the courts (Silverman, 2004).

### *C. The Confidentiality Risks*

In the broader context of e-commerce transactions, the requirement of confidentiality warrants that all communication between the trading parties to be restricted to the parties involved in that particular transaction, to the exclusion of intrusion by any third party who is not involved (Richmond, 1995). However, within the context of the courts, Sorell (1993-1994) contends that the duty to protect any confidential information is a challenging task as it might be in conflict with the public's right to access to it. Nonetheless, as Dore has correctly asserts that the final say

lies with the authority of the court to hold a certain data or information as being confidential and could only be made known among specific persons (Dore, 1978-1979). Accordingly, any infringement with the protected confidential information could lead to an infringement of the law and order, specifically within the setting of information submitted or revealed to the government offices including the courts (McCarthy and Kommeier, 1980-1981).

### D. The Data Integrity Risks

Finally, in relation to the basic control requirement of data integrity, Suh and Han (2003) contend that this requirement ensures that the data under transmission is not created, intercepted, modified or deleted illicitly. Similarly, Smedinghoff and Bro (1999) assert that such security control is concerned with the accuracy of data and completeness of the communication, providing confidence to a recipient before relying and acting on the message. Towards this end, Noblett et al suggest that it is essential to have a working policy to establish the chain of handling the data or information so as to ensure its integrity and usability (Noblett, Pollit and Presleym 2000). Nevertheless, as rightly argued by Cosic and Baca (2010) and Cavtat, Voyatzis and Pitas (1999), the emergence of ICT in the court processes could lead to the loss of control over the integrity of the data concerned.

## VII. Preliminary Findings

The research is currently at the data analysis stage, therefore, the complete findings have yet to be derived from the primary data. Nevertheless, a number of preliminary findings could be seen for the purpose of this paper.

Some of the respondents lack the awareness about the security risks entailing the ICT adoption at the courts. For instance, an interpreter of the court mentioned that she has no knowledge of any relative security risks of the ICT adoption. Meanwhile, for other respondents, although the security issue is acknowledged to be important, most of them downplayed the significance of security risks associated with ICT at the courts. In this respect, a solicitor of the High Court acknowledged the existence of the security risk, but at the same time affirmed that he was not concerned about it.

On the other hand, some respondents were under a misguided belief that the provision of a single layer security measure i.e. given user id and security password to access into the systems was perfectly adequate. A system developer of the ICT systems stated that security risk is not a primary concern. Similarly, a judge expressed his satisfaction with the security settings of the ICT at the courts and placing his total reliance on the system developer.

## VIII. Conclusion

Based on the discussion above, the adoption of the ICT at the High Courts in Malaysia has inevitably raised certain security implications. All these implications would in turn, have far reaching consequences not only on the way in which judicial business would be conducted but also on the way in which justice for the litigants would be delivered and constructed. It is pertinent to identify these implications so that the same could be addressed appropriately.

## Acknowledgement

We wish to thank Universiti Utara Malaysia and the Malaysian Ministry of Higher Education for financially supporting this research.

## References

[1] A. Aldridge, M. White, and K. Forcht, "Security considerations of doing business via the Internet: Cautions to be considered," *Internet Research: Electronic Networking Applications and Policy*, vol. 7, no. 1, pp. 9-15. 1997.

[2] J. N. Bailenson, J. Blaskovic, A. C. Beall, and B. Noveck, "Courtroom Applications of Virtual Environments, Immersive Virtual Environments, and Collaborative Virtual Environments," *Law and Policy*, vol. 28, no. 2, 2006.

[3] J. K. Bhatt, "Role of Information Technology in the Malaysian Judicial System: Issues and Current Trends," *International Review of Law Computers and Technology*, vol. 19, no. 2, pp. 199-208, 2005.

[4] Bhimani, A. Securing the Commercial Internet, Communications of the ACM, vol. 39, no. 6, pp. 29-35. 1996,

[5] M. B. Kirsten "Are Public Records Too Public – Why Personally Identifying Information should be removed from Both Online and Print Versions of Court Documents" *Ohio State Law Journal*, vol. 65, no, 1, pp. 413-450. 2004.

[6] C. Croatia, G. Voyatzis, and I. Pitas, "The Use of Watermarks in the Protection of Digital multimedia Products," in *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1197-1207, 1999.

[7] J. Chong, "A Primer on Digital Signature and Malaysia's Digital Signatures Act 1997," Computer Law and Security Report, vol. 14, no. 5, pp. 322-333, 1998.

[8] J. Cosic and B. Miroslav, "Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?" *International Conference on Information Technology Interfaces*, June 21-24, 2010.

[9] M. Dore, "Confidentiality Orders – The Proper Role of the Courts in Providing Confidential Treatment for Information Disclosed Through the Pre-Trial Discovery Process," New England Law Review, vol. 14, no. 1, 1978-1979.

[10] FitzGerald, T. Brian "Sealed v Sealed: A Public Court System Going Secretly Private," *Journal of Law and Politics*, pp. 381-414. 1989-1990.

[11] S. M. Furnell and T. Karweni, "Security implications of electronic commerce: A survey of consumers and businesses. Internet Research: Electronic Networking Applications and Policy," vol. 9, no. 5, pp. 372-382, 1999.

[12] D. Gefen, Electronic commerce: The role of familiarity and trust, Omega: The International Journal of Marketing Science, vol. 28, no. 6, pp. 725-737, 2000.

[13] H. M. Deril, "Contributions and Roles of the Court in the Development of E-Court" Round Table Conference on Transformation of Dispute Resolution Mechanism: Roles of the E-Court, Bangi, Selangor, Malaysia, 2011.

[14] Kuala Lumpur High Court, "CMS Briefing", Kuala Lumpur Courts Complex, 2010.

[15] K. McCarthy and J. W. Kornmeier, "Maintaining the Confidentiality of Confidential Business Information Submitted to the Federal Government," *36 Business Law Review*, 1980-1981.

[16] N. I. Abdullah, "New System to Speed Up Trials Four Times Faster", *the New Straits Times*, 2011.

[17] G. N. Michael, M. P. Mark, and A. P. Lawrence, "Recovering and Examining Computer Forensic Evidence," *Forensic Science Communications*, 2000.

[18] D. R. Richmond, "Key Issues in the Inadvertent Release and Receipt of Confidential Information," *72 Defense Counsel J*ournal, vol. 110, no. 1, pp. 110-120, 2005.

[19] S. S. Victoria "Are Public Records Really Public?: The Collision Between the Right to Privacy and the Release of Public Court Records over the Internet," (January 2000) Phoenix Law School, [Online]. Available: http://works.bepress.com/victoria_salzmann/8 accessed on 22 August 2011.

[20] M. S. Gregory "Rise of the Machines: Justice Information Systems and the Question of Public Access to Court Records over the Internet," *79 Washington Law Review*, vol. 175, no. 1, pp. 175-222, 2004.

[21] T. J. Smedinghoff, and R. H. Bro, "Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce," *J. Marshall J. Computer and Info. L*, vol. 17, no. 1, pp. 723-768, 1999.
[22] L. S. Sorell, "In-House Counsel Access to Confidential Information Produced During Discovery in Intellectual Property Litigation," *John Marshall Law Review*, vol. 27, no. 1, pp. 657, 1993-1994.
[23] B. Suh and I. Han, "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 135-161. 2003.
[24] R. West, "Tradition, Security Stall Court Technology" American City and County, 0149337X, Mar 2002.
[25] Z. Hamin, "What's Law Got To Do With It?: The Limits Of The Computer Crimes Act 1997 In Governing Computer Crimes Within The Malaysian Electronic Workplace", [2009] 4 MLJ cxci.
[26] Z. T. A. (Tun), "Using Technology to Improve Court Performance: Malaysia's Experience," Asia Pacific Judicial Reform Forum 2010, Beijing, 25-28 October 2010.